FAQ de segurança satisfeito: Como você alcança o CLI em uma ferramenta de segurança satisfeita?

Índice

Introdução

Este documento descreve como alcançar o CLI através de um cliente do telnet ou do Shell Seguro (ssh) em uma ferramenta de segurança do índice de Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco envia por correio eletrónico a ferramenta de segurança (o ESA)
- Ferramenta de segurança da Web de Cisco (WSA)
- Dispositivo do Gerenciamento do Cisco Security (S A)
- AsyncOS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ESA AsyncOS, todas as versões
- Cisco WSA AsyncOS, todas as versões
- Versões AsyncOS de Cisco S A, todas as versões

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Note: Este documento provê o software que não é mantido nem é apoiado por Cisco. A informação é fornecida como uma cortesia para sua conveniência. Para a assistência adicional, contacte por favor o fornecedor de software.

Como você alcança o CLI em uma ferramenta de segurança satisfeita?

Você pode alcançar o CLI de seu dispositivo com um cliente telnet ou um cliente SSH. Contudo, o protocolo telnet é unencrypted, assim que quando você registra em seu dispositivo com o telnet, suas credenciais enlata seja roubado mais facilmente.

Cisco recomenda que todas as máquinas da produção usam um cliente SSH. Adicionalmente, o cliente telnet de Microsoft Windows do padrão é difícil de usar-se. Pelo padrão de fábrica, o telnet é configurado na porta de gerenciamento.

Termine estas etapas a fim desabilitar o telnet:

1. Log na Web GUI.
2. Navegue à **rede > às interfaces IP**.
3. Clique o nome da relação que você quer editar.
4. Desmarcar a caixa de verificação do **telnet no** campo dos serviços.

Termine estas etapas a fim alcançar seu dispositivo com SSH (porta 22):

1. Instale um cliente SSH em Microsoft Windows, tal como a massa de vidraceiro.
2. Lance o cliente SSH:

   Adicionar a informação de host para seu dispositivo (tal como **c650.example.com**).

   Clique a **carga**.

   Dê entrada com o seu nome de usuário.

   Incorpore a sua senha.
3. Abra um comando prompt com ***nix**.
4. Incorpore o comando de **exampleC650.com do ssh $**.
5. Se você precisa de especificar um usuário diferente, incorpore o comando do **ssh <user>@exampleC650.com $**. Se o nome de usuário é **admin**, incorpore o comando de **admin@C650.example.com do ssh $**.

Termine estas etapas a fim alcançar seu dispositivo com o telnet:

> **Note**: Cisco recomenda que você usa um cliente SSH para o acesso; o uso do telnet não é recomendado.

1. Abra um comando prompt.
2. Incorpore o comando de **c650.example.com do telnet**.
3. Dê entrada com o seu nome de usuário.
4. Incorpore a sua senha.